NO.	HPCI-CA01-001E-09

User's Guide
HPCI Login Manual

Ver. 9

Nov. 11, 2014

Revision History

Date issued	Ver.	Description
2012.03.30	1	First Release
2012.06.06	2	In section "3.1.1 Download the Software Package", added the Globus Toolkit version In section "3.2.1 CentOS (5, 6)", modified the Globus Toolkit installation procedure
2012.08.20	3	Removed the MyProxyUploader procedures Modified the login procedure with GSI-SSHTerm for HPCI Added the section "2.5.1.1 Troubleshooting"
2012.08.29	4	Added a border line to the footer
2012.10.04	5	Removed the certificate downloading procedure Modified the number of Signing Policy files required to be downloaded Added the procedure for making the directory `.globus` for Windows users Unified the terminology to fit the 'Quick Start Guide'
2012.12.05	6	Changed the procedure for starting GSI-SSHTerm to double-click on Explorer In section "3.1.1 Download the Software Package", added the requirement of setting up Java for Windows users
2013.04.11	7	Updated the screen captures in sections "2.1 Obtaining a Certificate" and "2.2 Proxy Certificate Registration".
2014.07.29	8	Updated Fig. 4. In section "1.1 Overview", added how to get the maintenance and trouble information, and added the availability of `portal-c.hpci.nii.ac.jp` in case of trouble on `portal.hpci.nii.ac.jp`. In section "1.3 Operating Environment", added the environmental information of `portal-c.hpci.nii.ac.jp`. In sections "2.1.1 Issuing a Client certificate", "2.3.2.1 Troubleshooting" and "2.3.3.1 Troubleshooting", added the availability of `portal-c.hpci.nii.ac.jp` in case of trouble on `portal.hpci.nii.ac.jp`. In sections "2.1.1.1 Troubleshooting", "2.2.1.1 Troubleshooting", "2.3.1.1 Troubleshooting" and "2.3.3.1 Troubleshooting", changed the term 'system administrator' to 'HPCI Helpdesk'. In sections "2.3.3 Download with Globus Toolkit", "2.5.2 Login with Globus Toolkit (for Unix/Linux/MacOSX)" and "2.6.2 Transfer with Globus Toolkit (for Unix/Linux/MacOSX)", changed the filename of downloaded proxy certificate to 'x509up_u[UID]'. Added the troubleshooting in sections "2.3.3.1 Troubleshooting (4)", "2.3.3.1 Troubleshooting (5)", "2.4.1.1 Troubleshooting" and "2.5.1.1 Troubleshooting". In section "3.2.1 CentOS (5, 6)", added how to check the Globus Toolkit version to be installed.

		Added the section "5 Appendix". Modified the term 'HPCI Certificate Issue System' to 'HPCI Certificate Issuing System'. Replaced the platform dependent character '−' with the one-byte character '-'.
2014.11.11	9	In section "2.1.1 Issuing a Client certificate (1)", added how to bookmark HPCI Certificate Issuing System. In section "2.1.1 Issuing a Client certificate (2)", added the description of the link for switching language. Updated Fig. 2 and Fig. 3.

Document List

- Administrator's Guide Group
  - Administrator's Guide, HPCI Account IdP
  - Administrator's Guide, GSI-SSH Server
  - Administrator's Guide, Obtaining a Server Certificate
  - Administrator's Guide, Certificate Authority System
  - Administrator's Guide, Certificate Management System
  - Administrator's Guide, Certificate Issuing System
  - Administrator's Guide, Shibboleth DS
  - HPCI CA CPS
  - HPCI CA Certificate and CRL Profile
  - Administrator's Guide, HPCI Account IdP for Test Environment
  - Administrator's Guide, GSI-SSH Server for Test Environment
  - Administrator's Guide, Obtaining a Server Certificate for Test Environment
  - Administrator's Guide, Certificate Authority System for Test Environment
  - Administrator's Guide, Shibboleth DS for Test Environment
  - Administrator's Guide, HPCI Usage Manual
  - Administrator's Guide, Shibboleth SP
- User's Guide Group
  - User's Guide, HPCI Login Manual

Table of Contents

1. Introduction

1.1. Overview

This document is the Login Manual for the HPCI environment.

This document describes how to login to the login server for users of the HPCI computing and storage resources. Users need to perform the following steps:

- Obtain a certificate
  First, you need to obtain a client certificate to login (Single Sign On) to the HPCI environment. For details, refer to "2.1 Obtaining a Certificate".
- Obtain a proxy certificate
  Next, you need to obtain the proxy certificate generated from your client certificate to login (Single Sign On) to the HPCI environment. For details, refer to "2.2 Proxy Certificate Registration" and "2.3 Downloading the Proxy Certificate".
- Login and transfer files to the login server
  After obtaining the proxy certificate, you can login and transfer files to the login server. For details, refer to "2.5 Login to the Login Server" and "2.6 Transferring files to the Login Server".
- Install and configure necessary applications
  You need to install several applications to login to the login server. For details, refer to "3 Appendix: Installing applications".

In order to login to the HPCI environment, you must have already acquired an HPCI-ID. You are also required to be a member of an approved research project and have an HPCI account.

You can check information about the maintenance and trouble, by the mail from HPCI Helpdesk or at the web page "国立情報学研究所 > 運用情報" on HPCI Contents Management System for Information Sharing.
If you cannot access HPCI Certificate Issuing System (`portal.hpci.nii.ac.jp`) due to system failure, you can try to access an alternative system (`portal-c.hpci.nii.ac.jp`) instead. However, availability of the service is depending on seriousness of trouble.

> HPCI Contents Management System for Information Sharing
> `https://www.hpci-office.jp/info/`

In this document, **bold** characters in the command image are the commands you need to execute.
'%': run the command as the privileged user `root` in Unix/Linux/MacOSX
'$': run the command as a non-privileged user (not `root`) in Unix/Linux/MacOSX
'C:¥>': run the command in the command prompt on Windows

1.2. Flow

The numbers in the following figure correspond to the section numbers in this document (Fig. 1).

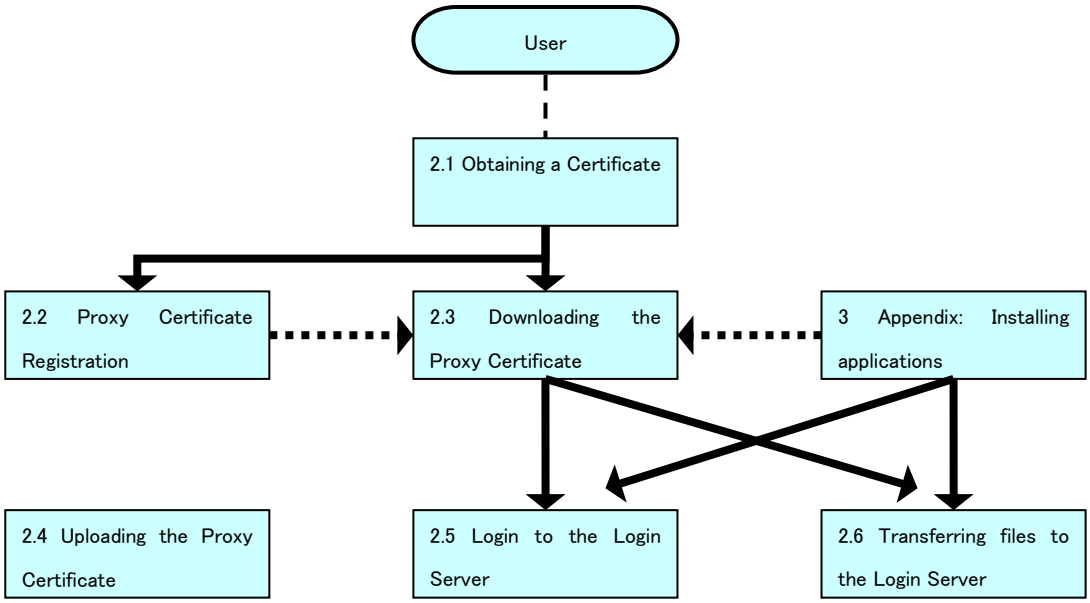
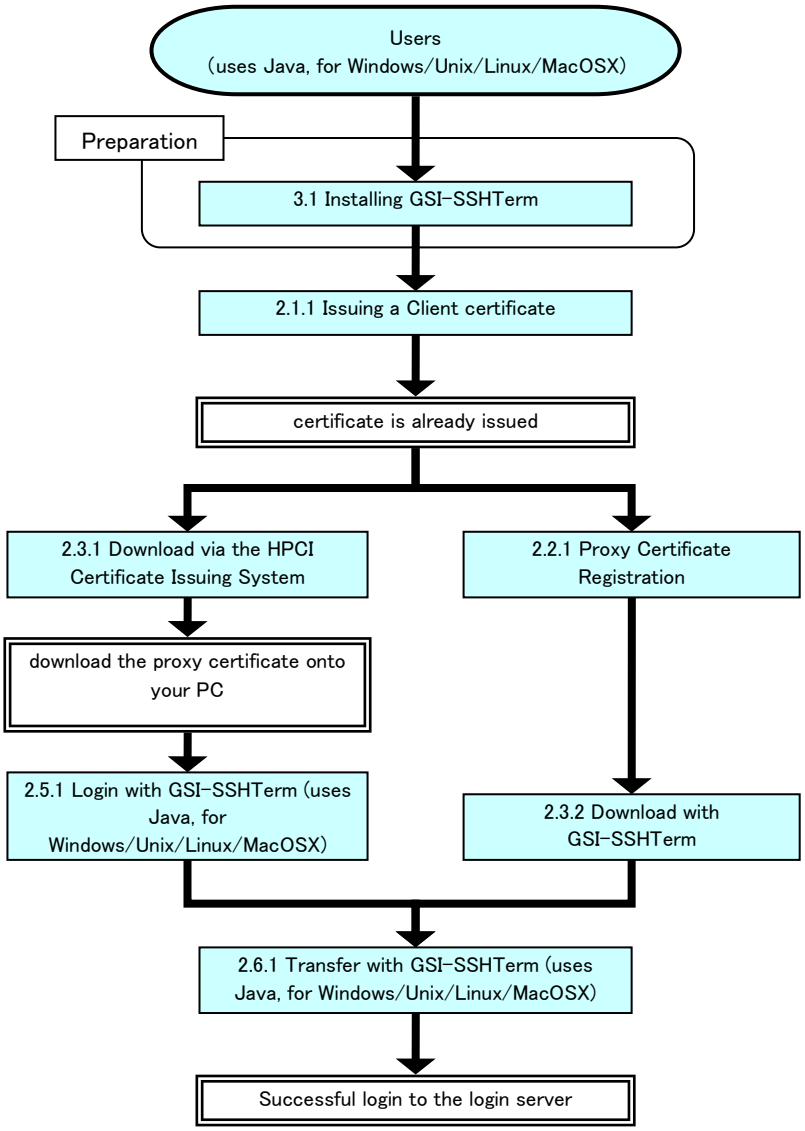


Fig. 1

In order to login to the login server, you need to perform the following steps:

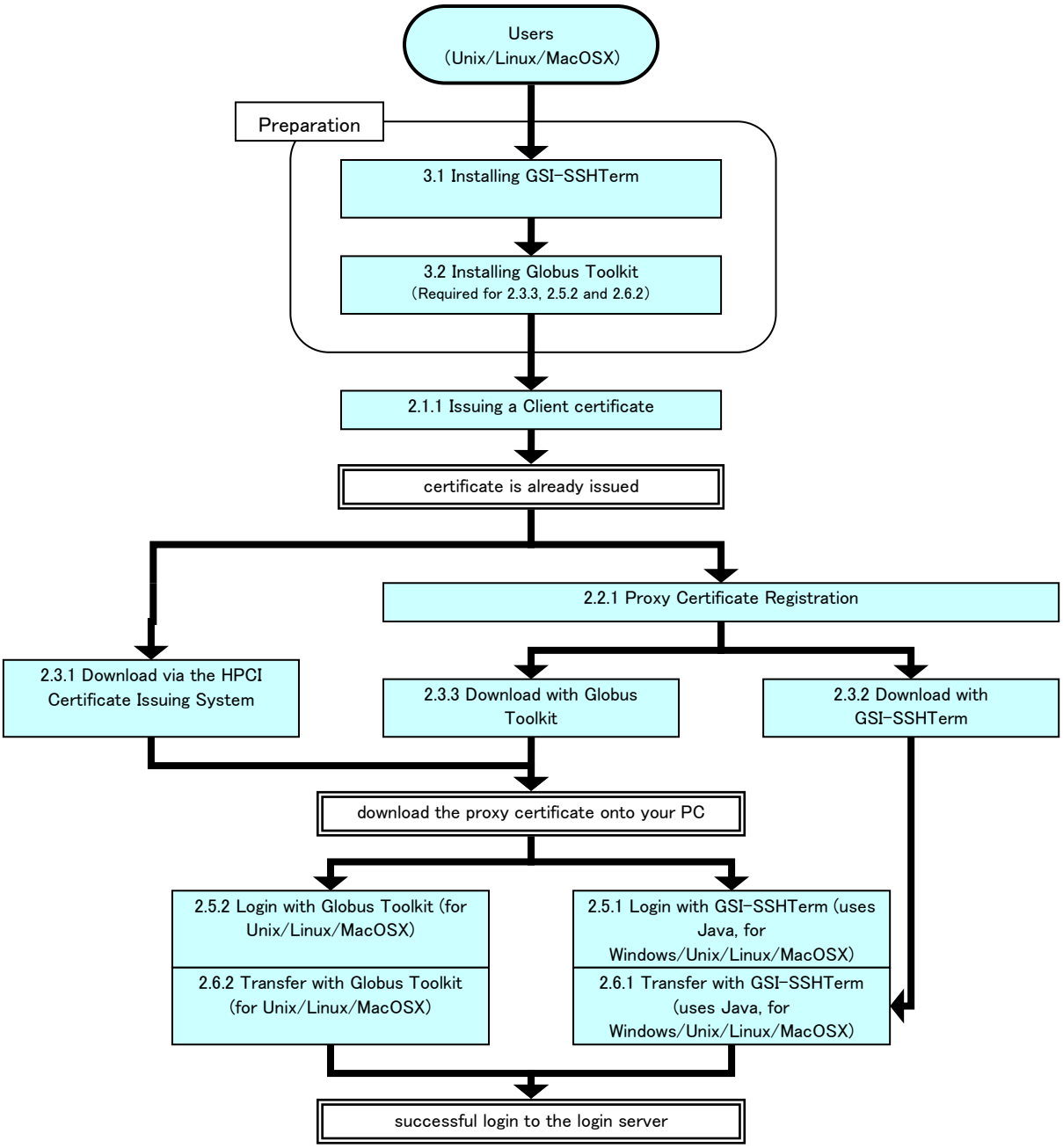
- For Windows/Unix/Linux/MacOSX

(1) 2.1.1 Issuing a Client certificate
(2) 2.2.1 Proxy Certificate Registration
(3) 2.3.2 Download with GSI-SSHTerm
(4) 2.6.1 Transfer with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)



- For Unix/Linux/MacOSX, using the command line

(1) 2.1.1 Issuing a Client certificate
(2) 2.3.1 Download via the HPCI Certificate Issuing System
(3) 3.2 Installing Globus Toolkit
(4) 2.5.2 Login with Globus Toolkit (for Unix/Linux/MacOSX)
(5) 2.6.2 Transfer with Globus Toolkit (for Unix/Linux/MacOSX)



1.3. Operating Environment

- Browser: Firefox 7 or later, Internet Explorer 6 or later, Safari 5, Google Chrome 18
- GSI-SSHTerm: Windows XP/Vista 32bit, Windows 7 32/64bit, Linux (CentOS 6 32bit, Ubuntu 12.04TLS, openSUSE 12.2), Mac OS X (10.6, 10.7, 10.8.2)
- Globus Toolkit: Linux (CentOS 5, 6 32bit), Mac OS X (10.6, 10.7, 10.8.2)

You need to open the following ports.

【Firewall configuration】

TCP /UDP	Source address	Source port	Destination address	Destination port	Comments
TCP	[client host]	ANY	[CA repository]	80 443	Required to get information from the HPCI CA (Certificates, CRL) (refer to 3)
TCP	[client host]	ANY	[Shibboleth DS]	443	Required for Shibboleth authentication (refer to 2.1.1)
TCP	[client host]	ANY	[IdP server of the Primary Center]	443	Required for Shibboleth authentication (refer to 2.1.1)
TCP	[client host]	ANY	[HPCI Certificate Issuing System]	443	Required for access to the HPCI Certificate Issuing System (refer to 2.1.1)
TCP	[client host]	ANY	[HPCI Certificate Issuing System]	7512	Required for Uploading and downloading the proxy certificates (refer to 2.3 and 2.4)
TCP	[client host]	ANY	[Login Server]	2222	gsissh, gsiscp (refer to 2.5 and 2.6)
UDP	[client host]	ANY	[DNS server]	53	DNS
UDP	[client host]	123	[NTP server]	123	NTP

As of 1October 2012, use the following configuration information.

Server	IP address
[CA repository]	136.187.100.132 (www.hpci.nii.ac.jp)
[Shibboleth DS]	136.187.100.134 (ds.hpci.nii.ac.jp)
[HPCI Certificate Issuing System]	136.187.100.135 (portal.hpci.nii.ac.jp) 157.1.137.20 (portal-c.hpci.nii.ac.jp)
[IdP server of the Primary Center]	URL reached through the following steps: (1) Access the HPCI Certificate Issuing System with your Web browser. (2) Select your Primary Center on the Primary Center Selection screen, and then (3) be automatically redirected to the Login for Primary Center screen.
[Login Server]	IP address of the login server. Please contact the HPCI system providers, or check the HPCI office website for the correct address.
[DNS server]	ask your system administrator
[NTP server]	ask your system administrator

2. Usage

2.1. Obtaining a Certificate

You need to obtain your client certificate in order to login to the HPCI resources using Single Sign On (SSO). All certificates have an expiration date, and you will need to go through this process again to re-issue the certificate once it expires.

This chapter describes how to obtain a client certificate.

2.1.1. Issuing a Client certificate

(1) Access the HPCI Certificate Issuing System.

HPCI Certificate Issuing System
`https://portal.hpci.nii.ac.jp/`

If you cannot access `portal.hpci.nii.ac.jp`, refer to the section "1.1 Overview", and access an alternative system, `portal-c.hpci.nii.ac.jp`.

If you want to bookmark the URL of HPCI Certificate Issuing System, please do it after successful login (Fig. 4). Because the URL of Primary Center Selection screen (Fig. 2) is generated each time of your access, the bookmark may be useless.

(2) You will be automatically redirected to the Primary Center Selection screen (Fig. 2). Select the Primary Center that you chose when you registered the HPCI-ID, and click the Select button. Once the Login for Primary Center screen appears (Fig. 3), enter your HPCI account information, and click the "ログイン" button. You can switch language of the text on the screen by clicking the link "Change language to English" or "日本語に切り替え".

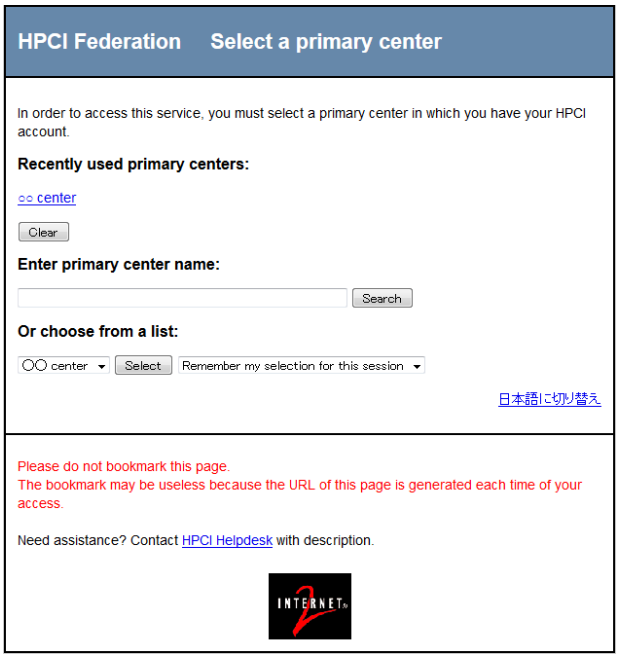


Fig. 2

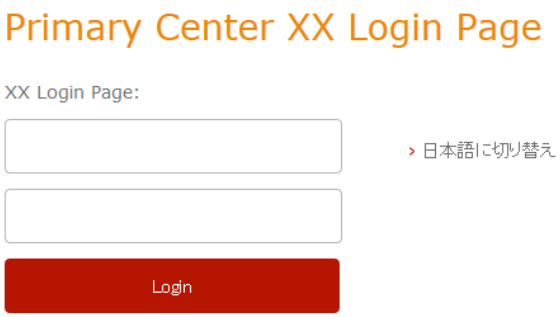


Fig. 3

(3) The HPCI Certificate Issuing System screen is displayed (Fig. 4) after successfully logging in to the HPCI Certificate Issuing System.

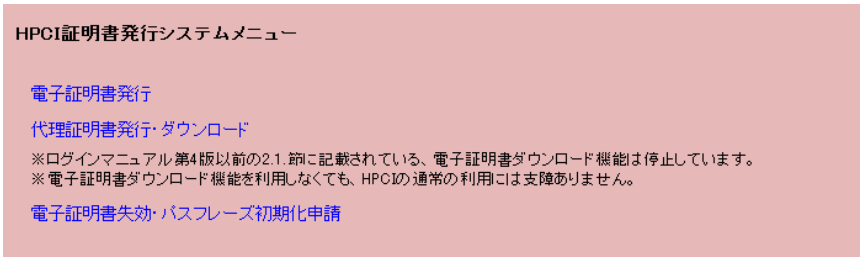


Fig. 4

(4) Click on the "電子証明書発行" link to display the "電子証明書発行" form

◆ If you issue a certificate the certificate for the first time

The "電子証明書発行" screen should look like Fig. 5.

Fig. 5

◆ If you have already issued the certificate

The "電子証明書発行" screen should look like Fig. 6.

Fig. 6

(5) At the "電子証明書発行" screen (Fig. 5),(Fig. 6), enter the private key passphrase required for issuing the certificate, and click the "発行" button.

◆ If you issue a certificate the certificate for the first time

On the entry form, you must enter the new passphrase in the "新しい電子証明書のパスフレーズ" fields. Passphrases longer than 12 characters are highly recommended. The Maximum length for passphrases is 20 characters.

The passphrase you entered here will be required when you issue the proxy certificate as described in section 2.2 Proxy Certificate Registration and 2.3 Downloading the Proxy Certificate.

◆ If you have already issued the certificate

On the entry form, you must enter the old passphrase in the "現在の電子証明書のパスフレーズ" field.

And you must enter the new passphrase in the "新しい電子証明書のパスフレーズ" fields. Passphrases longer than 12 characters are highly recommended. The Maximum length for passphrases is 20 characters.

The passphrase you entered here will be required when you issue the proxy certificate as described in section 2.2 Proxy Certificate Registration and 2.3 Downloading the Proxy Certificate.

(6) The "電子証明書発行完了" screen is displayed (Fig. 7) when your certificate has been successfully issued.

Fig. 7

Your certificate is stored in the repository on the HPCI Certificate Management System.

You do not need to do the above procedure again until after the expiration date of your client certificate.

You need to download the proxy certificate generated with your client certificate to access to the login server. Proceed to the section "2.3 Downloading the Proxy Certificate".

2.1.1.1. Troubleshooting

(1) Troubleshooting for the error message "新しい電子証明書のパスフレーズを入力してください。"

The error message "新しい電子証明書のパスフレーズを入力してください。" is shown on the "電子証明書発行情報入力" screen (Fig. 5, Fig. 6), when you have clicked the "発行" button without entering a passphrase in the entry form (Fig. 8).

Fig. 8

Enter a passphrase, and try again.

(2) Troubleshooting for the error message "6 文字以上入力してください。"

The error message "6 文字以上入力してください。" is shown on the "電子証明書発行情報入力" screen (Fig. 5, Fig. 6), when you have clicked the "発行" button after entering passphrases consisting of less than six characters (Fig. 9).

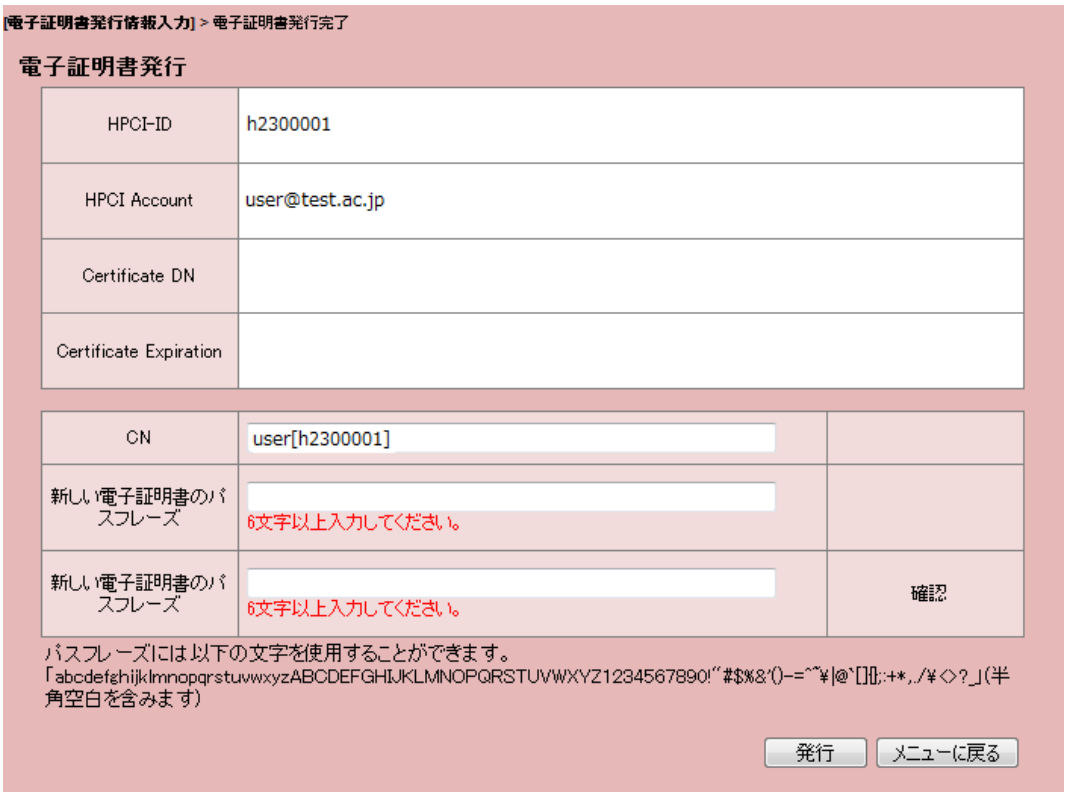


Fig. 9

Enter a passphrase consisting of six characters or more (more than 12 characters are recommended), and try again.

(3) Troubleshooting for the error message "20 文字以下入力してください。"

The error message "20 文字以下入力してください。" is shown on the "電子証明書発行情報入力" screen (Fig. 5, Fig. 6), when you have clicked the "発行" button after entering passphrases consisting of more than 20 characters (Fig. 10).

Fig. 10

Enter a passphrase consisting of 20 characters or less, and try again.

(4) Troubleshooting for the error message "新しい電子証明書のパスフレーズが一致しません。"

The error message "新しい電子証明書のパスフレーズが一致しません。" is shown on the "電子証明書発行情報入力" screen (Fig. 5, Fig. 6), when you have clicked the "発行" button after entering two passphrases that do not match (Fig. 11).

Fig. 11

Make sure you have entered the same passphrase in both boxes, and try again.

(5) Troubleshooting for the error message "現在の電子証明書のパスフレーズが正しくありません"

The error message "現在の電子証明書のパスフレーズが正しくありません" is shown on the "電子証明書発行情報入力" screen (Fig. 6), when you have clicked the "発行" button after entering an incorrect old client certificate passphrase (Fig.12).

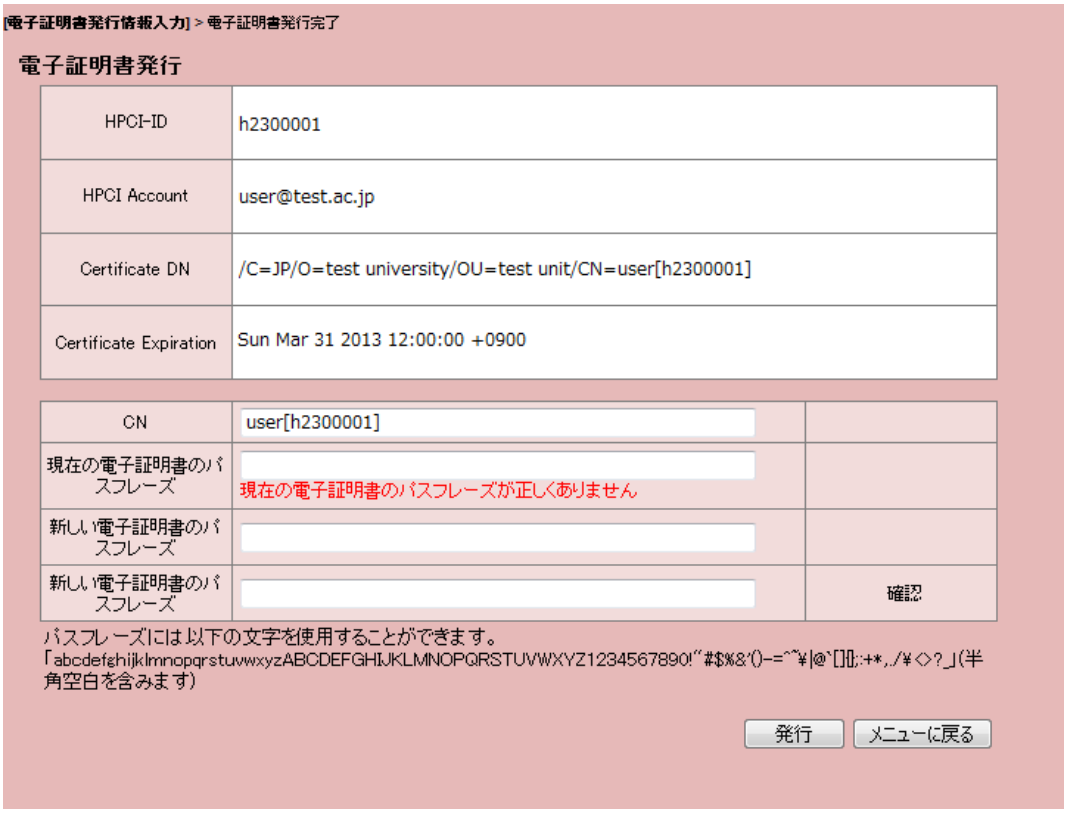


Fig.12

Check the passphrase, and try again.

(6) Troubleshooting for the error message "システムエラーが発生しました。"

When the error message "システムエラーが発生しました。" is displayed on the screen (Fig. 13), please contact HPCI Helpdesk (`https://www.hpci-office.jp/contact/index.html`) and send the message and the error code.

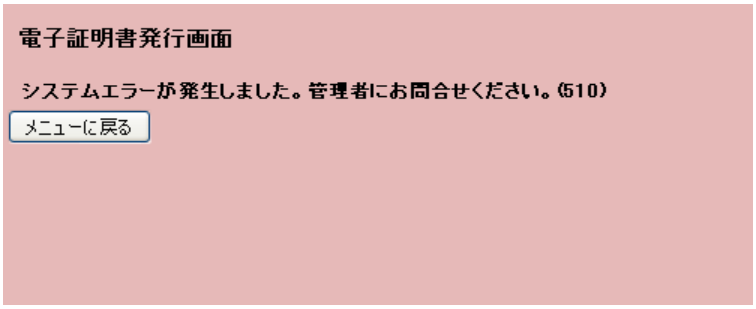


Fig. 13

2.2. Proxy Certificate Registration

You can skip this section if you will download your proxy certificate from the HPCI Certificate Issuing System as described in section "2.3 Downloading the Proxy Certificate".

The section "5.1 Flow of Proxy Certificate Registration and Downloading" describes the difference of proxy certificate registration and downloading.

2.2.1. Proxy Certificate Registration

(1) Access the HPCI Certificate Issuing System.

For details, refer to 2.1.1.

(2) On the "HPCI 証明書発行システムメニュー" screen, click the "代理証明書発行" link. This will bring you to the "代理証明書発行" form (Fig. 14).

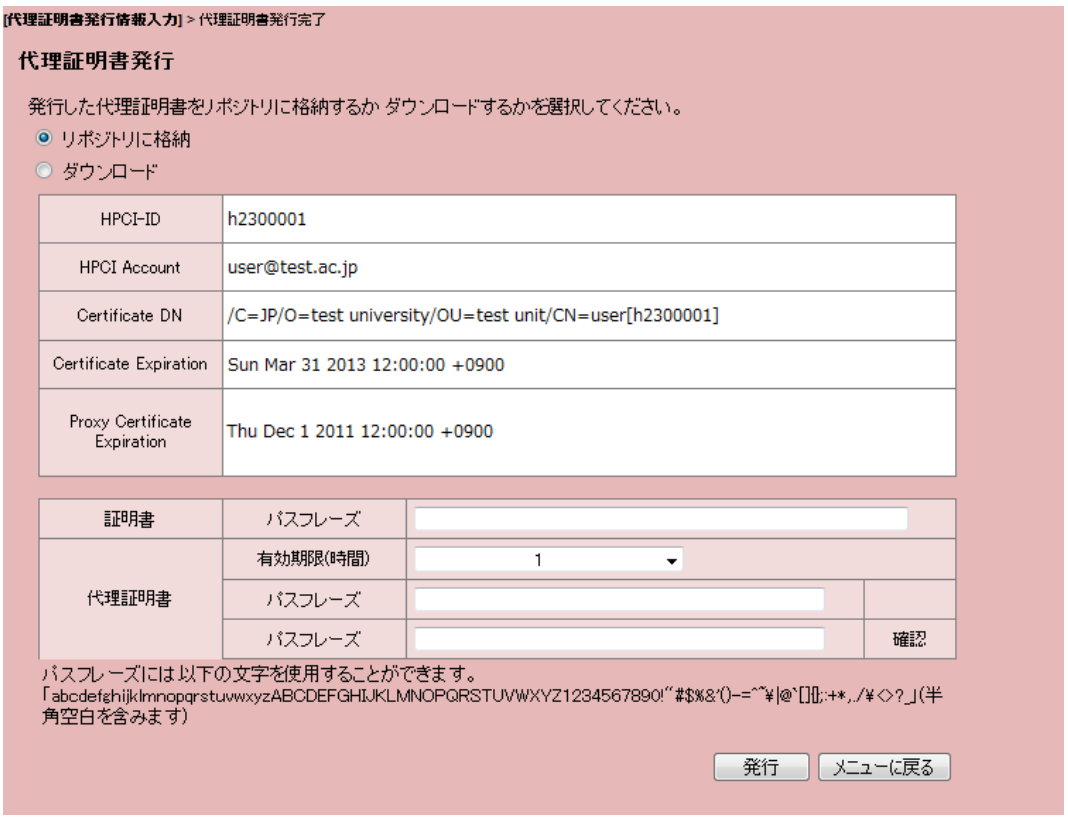


Fig. 14

Click the "リポジトリに格納" radio button, fill in the "証明書", "有効期限" and "パスフレーズ" fields, and click the "発行" button to store the Proxy Certificate in the proxy certificate repository.

- 証明書 - パスフレーズ（your client certificate passphrase）
- 代理証明書 - 有効期限（select a term of validity (in hours) for the proxy certificate you are going to register）
- 代理証明書 - パスフレーズ（passphrase required when you obtain the proxy certificate from the repository）
- 代理証明書 - パスフレーズ - 確認(same passphrase as the above）

(3) The "代理証明書発行完了" screen is displayed (Fig. 15) when your proxy certificate has been successfully registered.

Fig. 15

The Proxy Certificate is stored in the repository.

2.2.1.1. Troubleshooting

(1) Troubleshooting for the error message "パスフレーズを入力してください。"

The error message "パスフレーズを入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 14), when you have clicked the "発行" button without entering anything into the "証明書パスフレーズ" or "代理証明書パスフレーズ" fields in the entry form (Fig. 16)

Fig. 16

Enter the required passphrases, and try again.

(2) Troubleshooting for the error message "6 文字以上入力してください。"

The error message "6 文字以上入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 14), when you have clicked the "発行" button after entering a passphrase consisting of less than six characters (Fig. 17).

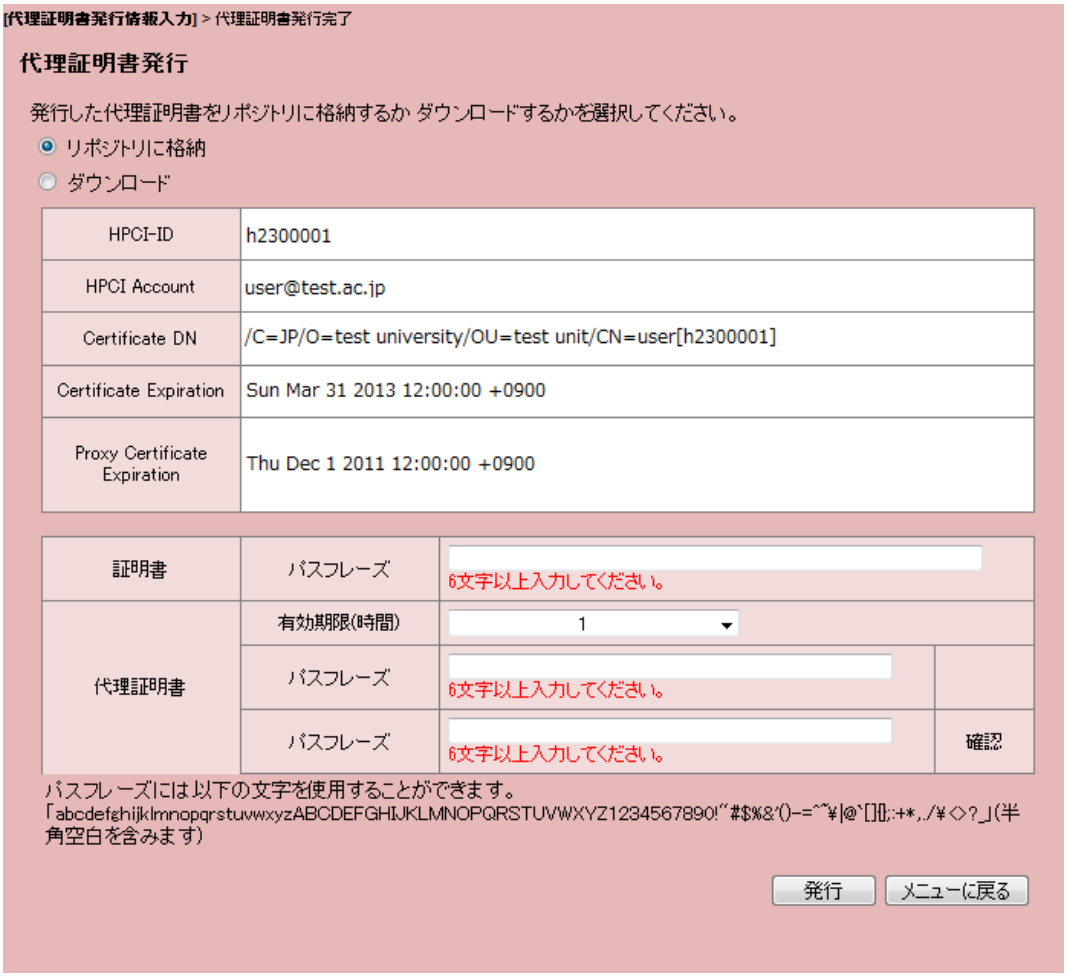


Fig. 17

Enter a passphrase consisting of six characters or more (more than 12 characters are recommended), and try again.

(3) Troubleshooting for the error message "20 文字以下入力してください。"

The error message "20 文字以下入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 14), when you have clicked the "発行" button after entering a passphrase consisting of more than 20 characters (Fig. 18).

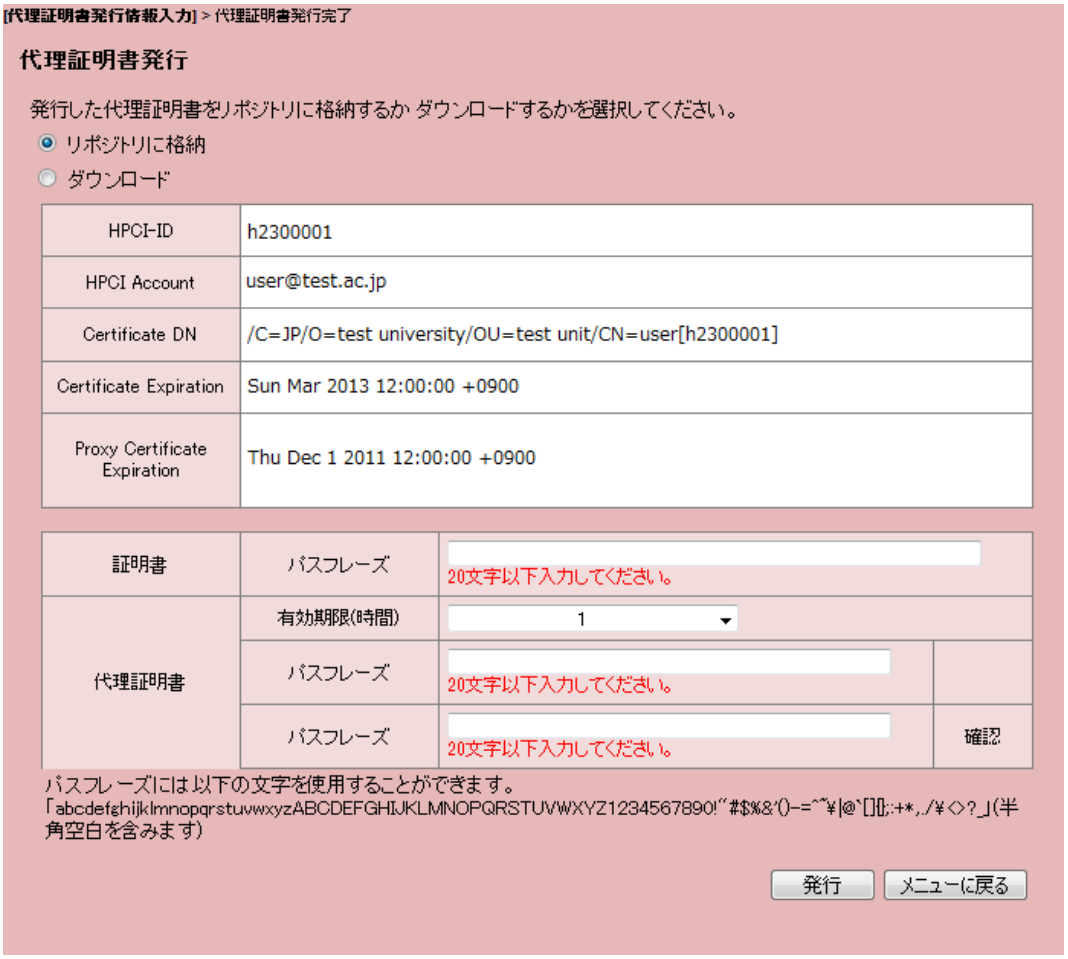


Fig. 18

Enter a passphrase consisting of 20 characters or less, and try again.

(4) Troubleshooting for the error message "パスフレーズが間違っています。"

The error message "パスフレーズが間違っています。" is shown on the "代理証明書ダウンロード" screen (Fig. 14), when you have clicked the "発行" button after entering an incorrect client certificate passphrase (Fig. 19).

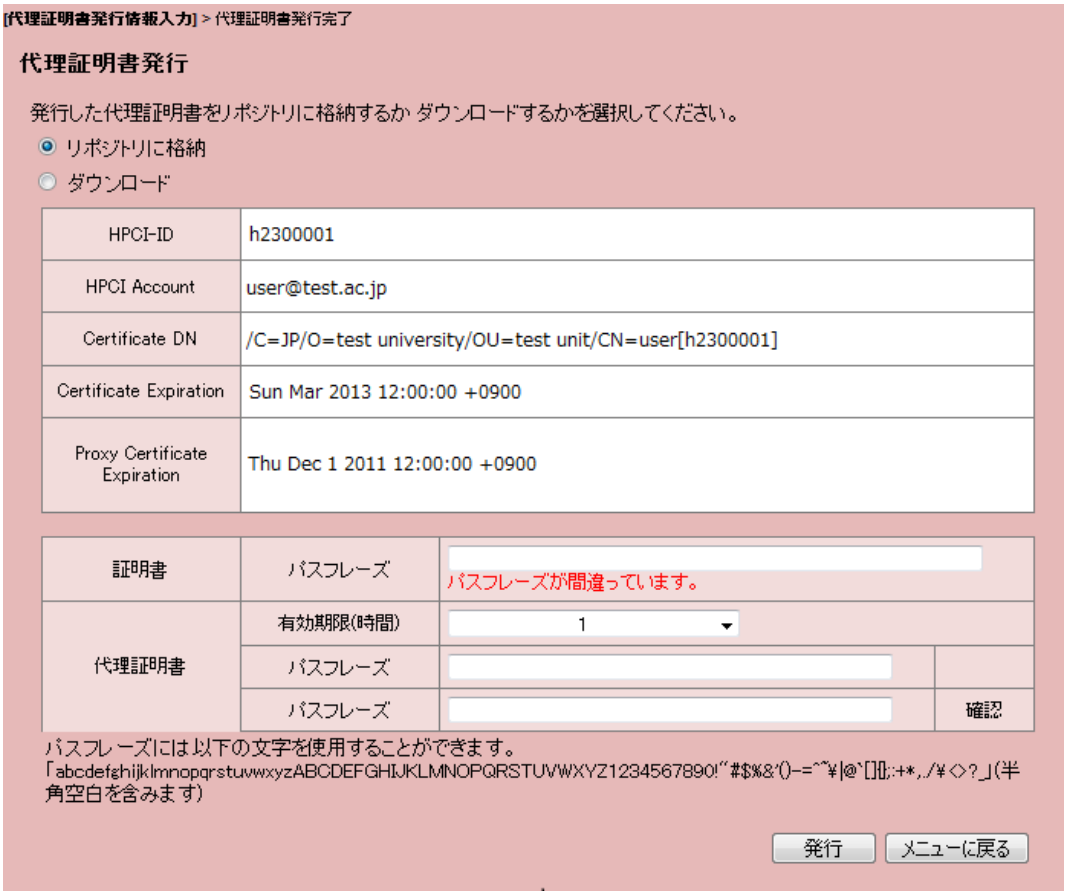


Fig. 19

Check the passphrase, and try again.

(5) Troubleshooting for the error message "パスフレーズが一致しません。" for the Proxy certificate

The error message "パスフレーズが一致しません。" is shown on the "代理証明書発行情報入力" screen (Fig. 14), when you have clicked the "発行" button after entering two passphrases for the Proxy Certificate that do not match (Fig. 20).

Fig. 20

Make sure you have entered the same passphrase in both boxes, and try again.

(6) Troubleshooting for the error message "システムエラーが発生しました。"

When the error message "システムエラーが発生しました。" is shown on the screen (Fig. 21), please check the error code.
If the error code is "**526:code(-3)**", your certificate may have expired

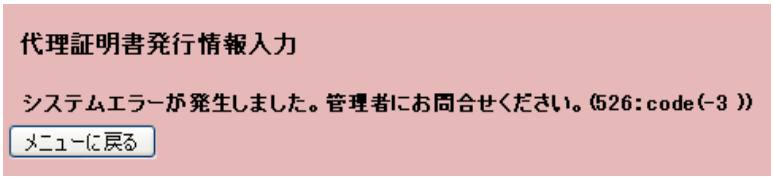


Fig. 21

Renew your client certificate, and try again.

Please contact HPCI Helpdesk (`https://www.hpci-office.jp/contact/index.html`) regarding other error codes.

2.3. Downloading the Proxy Certificate

This section describes the three procedures necessary for downloading the proxy certificate from the repository. Select the one which is suitable for your client environment.

OS	2.3.1 Download via the HPCI Certificate Issuing System	2.3.2 Download with GSI-SSHTerm	2.3.3 Download with Globus Toolkit
Windows	OK	OK	NG
Mac OS X	OK	OK	OK
Linux	OK	OK	OK
	Web browser required	Java is required	gcc is required

The section "5.1 Flow of Proxy Certificate Registration and Downloading" describes the difference of proxy certificate registration and downloading.

2.3.1. Download via the HPCI Certificate Issuing System

You do not need to complete the procedures in section "2.2 Proxy Certificate Registration" if you download the proxy certificate from the HPCI Certificate Issuing System as described in this section.

(1) Access the HPCI Certificate Issuing System.

For details, refer to section 2.1.1.

(2) Click the "代理証明書発行" link to display the "代理証明書発行" screen (Fig. 22).

Fig. 22

Click the "ダウンロード" radio button, fill in the "証明書-パスフレーズ" and "代理証明書-有効期限" fields, and click the "発行" button to download the Proxy Certificate from the proxy certificate repository.

- 証明書 - パスフレーズ (your client certificate passphrase)
- 代理証明書 - 有効期限 (select a term of validity (in hours) for the proxy certificate you are going to register)

(3) The "代理証明書発行完了" screen is displayed (Fig. 23) when your proxy certificate has been successfully issued.

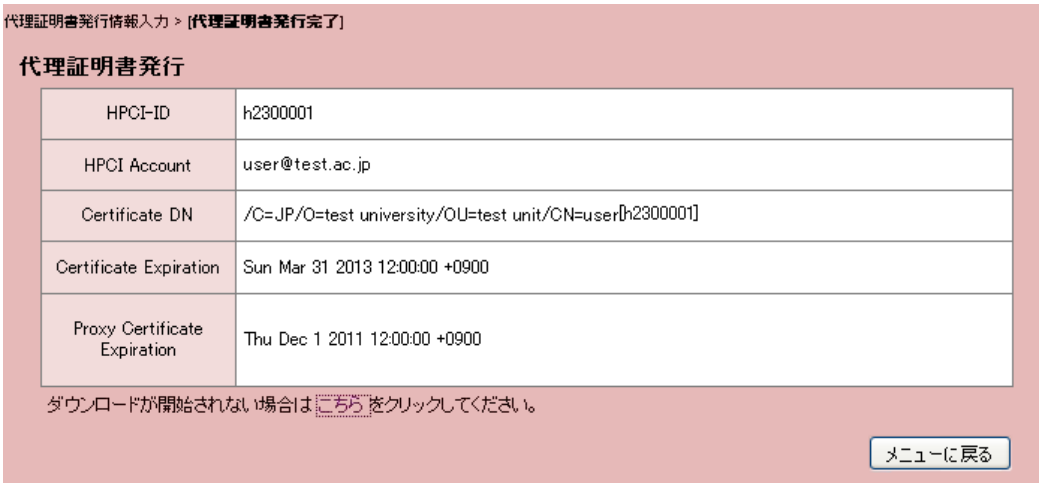


Fig. 23

After the "代理証明書発行完了" screen is displayed (Fig. 23), the download dialog appears. Save the proxy certificate with a name following the naming rule in Table 1. On Unix/Linux/MacOSX, set the proxy certificate file permissions to 600 in order to avoid `gsissh` errors.

Table 1

OS	Folder/Directory	File Name
Windows XP/Vista/7	%TMP% (*1)	x509up_u_**%USERNAME%** (*2)
Unix/Linux/MacOSX	/tmp	x509up_u**$UID**

(*1) To show the environment variables (%TMP%) on Windows, refer to the following table.

OS	To show the environment variables
Windows XP	My Computer > Properties > Advanced > Environment variables If TMP exists as both a System and User variable, use the User variable. (User Variables override System variables.)
Windows Vista/7	Start > Control Panel > Advanced stem settings > Advanced > Environment Variables If TMP exists as both a System and User variable, use the User variable. (User Variables override System variables.)

(*2) To show the environment variables %TMP% and %USERNAME% on Windows, run the following commands at the command prompt.

```
C:¥> echo %TMP%
C:¥DOCUME~1¥user¥LOCALS~1¥Temp¥9          ←display the value of %TMP%

C:¥> echo %USERNAME%
user                                      ←display the value of %USERNAME%
```

◆ Internet Explorer 6 on Windows XP

If you use Internet Explorer 6 on Windows XP, the following dialog appears (Fig. 24). Select "ファイルを保存する" and save the certificate with a name following the naming rule in Table 1.

Fig. 24

◆ Internet Explorer 9 on Windows 7

If you use Internet Explorer 9 on Windows 7, the following dialog appears on the bottom of the screen (Fig. 25). Click the ▼ button to the right of the "保存" button, select "名前を付けて保存", and download the certificate using a name following the naming rule in Table 1.

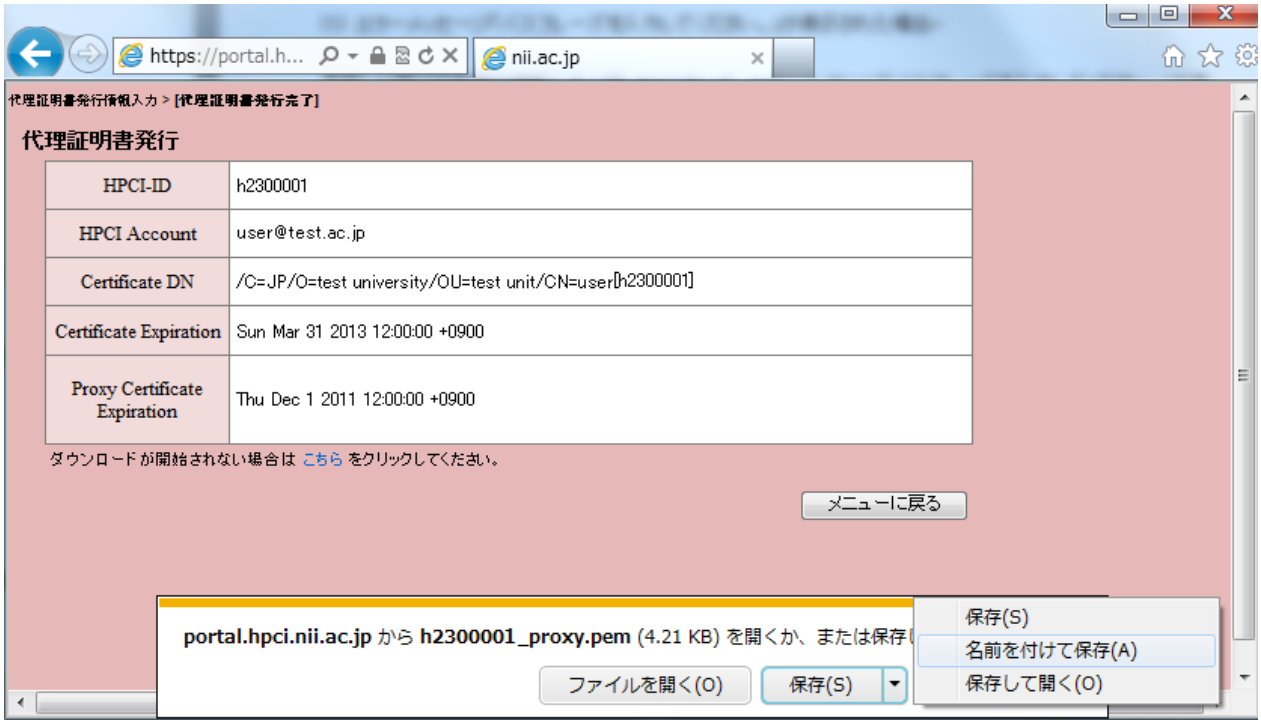


Fig. 25

If the above dialog (Fig. 24 or Fig. 25) does not appear, click the "こちら" link on the "代理証明書発行" screen (Fig. 23) to display the dialog.

Proceed to section "2.5 Login to the Login Server" to access the login server.

2.3.1.1. Troubleshooting

(1) Troubleshooting for the error message "パスフレーズを入力してください。"

The error message "パスフレーズを入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 22), when you have clicked the "発行" button without entering anything into the "証明書パスフレーズ" box in the entry form (Fig. 26)

Fig. 26

Enter a passphrase, and try again.

(2) Troubleshooting for the error message "6 文字以上入力してください。"

The error message "6 文字以上入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 22), when you have clicked the "発行" button after entering a passphrase consisting of less than six characters (Fig. 27).

Fig. 27

Enter a passphrase consisting of six characters or more (more than 12 characters are recommended), and try again.

(3) Troubleshooting for the error message "20 文字以下入力してください。"

The error message "20 文字以下入力してください。" is shown on the "代理証明書発行情報入力" screen (Fig. 22), when you have clicked the "発行" button after entering a passphrase consisting of more than 20 characters (Fig. 28).

Fig. 28

Enter a passphrase consisting of 20 characters or less, and try again.

(4) Troubleshooting for the error message "パスフレーズが間違っています。"

The error message "パスフレーズが間違っています。" is shown on the "代理証明書ダウンロード" screen (Fig. 22), when you have clicked the "発行" button after entering an incorrect client certificate passphrase (Fig. 29).

Fig. 29

Enter the correct passphrase, and try again.

(5) Troubleshooting for the error message "システムエラーが発生しました。"

When the error message "システムエラーが発生しました。" is shown on the screen (Fig. 30), please check the error code.
If the error code is "**526:code(-3)**", your certificate may have expired

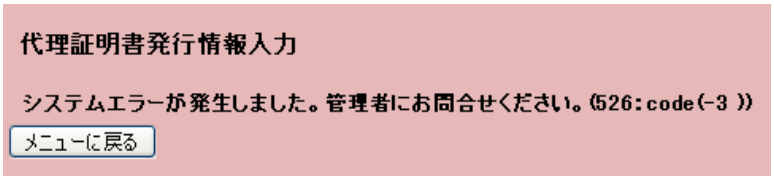


Fig. 30

Renew your client certificate, and try again.

Please contact HPCI Helpdesk (`https://www.hpci-office.jp/contact/index.html`) regarding any other error codes.

2.3.2. Download with GSI-SSHTerm

This subsection describes the procedure for downloading your Proxy Certificate using the MyProxy client function of GSI-SSHTerm.

Please refer to section "3.1 Installing GSI-SSHTerm" for instructions on installing the software, and refer to section "2.2 Proxy Certificate Registration" for instructions on registering of your proxy certificate.

(1) Start GSI-SSHTerm.

- Windows
  → Run Explorer, change directory to `bin`, and double-click on the file `sshterm.bat`.
- Unix/Linux/MacOSX
  → Change directory to `bin`, run `sshterm.sh`.

GSI-SSHTerm has successfully started if the following screen appears (Fig. 31).

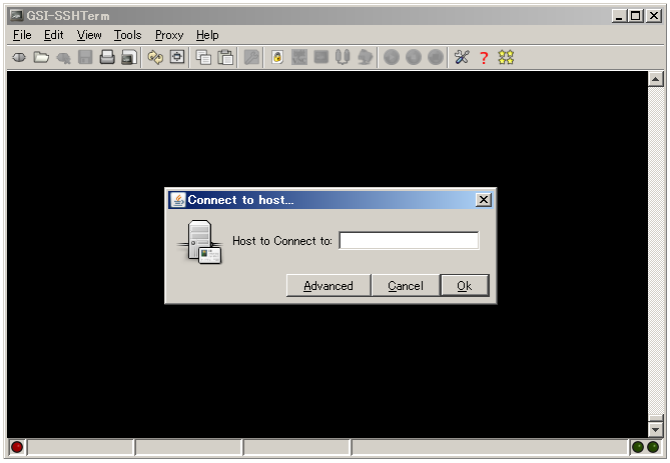


Fig. 31

If the screen above (Fig. 31) does not appear and GSI-SSHTerm does not start on Windows, check your Java settings (refer to section "3.1.1").

(2) Download the proxy certificate from the proxy certificate repository, and login to the login server.

Enter the hostname of the login server and click the OK button. The hostname of the login server should have been provided by the HCPI system providers that issued your HPCI local account. You do not need to click the 'Advanced' button. After clicking the OK button, the 'Grid Certificate/Proxy needed for Authentication' dialog appears (Fig. 32). In the dialog, enter the following information:

Fig. 32

- Hostname: `portal.hpci.nii.ac.jp`
- Account Name: your HPCI-ID, not your HPCI account nor your HPCI local account
- Passphrase: the passphrase you specified when registering the proxy certificate

After you enter the correct information, click the button 'Use MyProxy'. Your proxy certificate will be automatically downloaded, and you can login to the login server automatically. The proxy certificate is valid for 12 hours.

The downloaded proxy certificate is stored automatically as shown in the table below (Table 2).

Table 2

OS	Folder	Filename
Windows XP/Vista/7	%TMP% (*1)	x509up_u_**%USERNAME%** (*2)
Unix/Linux/MacOSX	/tmp	x509up_u**$UID**

(*1) (*2) To show the environment variables (%TMP% and %USERNAME%) on Windows, refer to section "2.3.1 (3)".

Your proxy certificate download is now complete. If you want to see the details of the downloaded proxy certificate, select 'Proxy > Proxy Info' from the menu (Fig. 33).

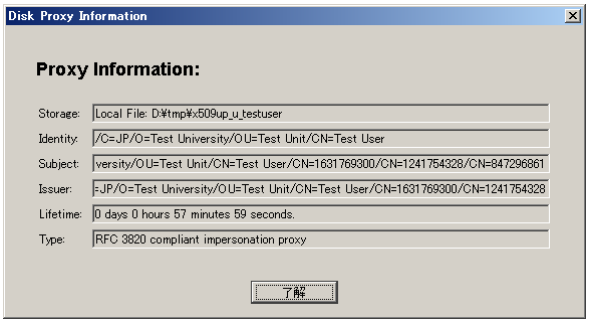


Fig. 33

(3) When you exit GSI-SSHTerm, you have to choose whether you want to delete the downloaded proxy certificate (Fig. 34).

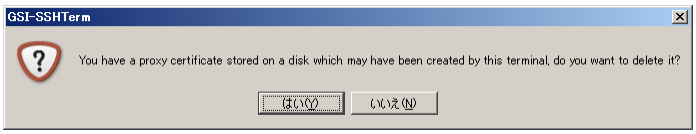


Fig. 34

If you want to delete the proxy certificate, click the 'はい' button, otherwise click the 'いいえ' button.

In general, click the 'いいえ' button to leave the proxy certificate on the client machine. By doing this, GSI-SSHTerm uses this proxy certificate next time, and you can login to the login server by simply entering the hostname of the login server in the 'Connect to host …' dialog (Fig. 31).

If you do not want to leave the proxy certificate on the client machine, click the 'はい' button to delete the proxy certificate. In this case, refer to section '2.3.2' if you need to download the proxy certificate again.

2.3.2.1. Troubleshooting

(1) Troubleshooting for the error message "Problem while accessing MyProxy. MyProxy get failed."

The error message " Problem while accessing MyProxy. MyProxy get failed." (Fig. 35) is shown under any of the following conditions:

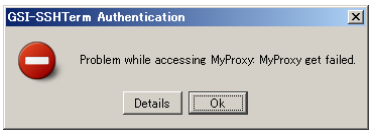


Fig. 35

A) The hostname of the proxy certificate repository is incorrect
→ Enter the correct hostname, and try again.

B) A trouble occurs at HPCI Certificate Issuing System (`portal.hpci.nii.ac.jp`)
→Refer to "1.1 Overview", and use `portal-c.hpci.nii.ac.jp` instead.

C) The proxy certificate stored in the repository has expired
→ Refer to "2.2 Proxy Certificate Registration" and "2.3.2", and try again.

D) The HPCI-ID you entered is incorrect
→ Enter the correct HPCI-ID, and try again.

(2) Troubleshooting for the error message "MyProxy: Password must be at least 6 characters long."

The error message "MyProxy: Password must be at least 6 characters long." is shown when you have clicked the 'Use MyProxy' button after entering passphrases consisting of less than six characters (Fig. 36).

Fig. 36

Check the passphrase, and try again.

(3) Troubleshooting for the error message "MyProxy: Bad username and/or password"

The error message "MyProxy: Bad username and/or password" is shown when you have entered an incorrect HPCI-ID or passphrase (Fig. 37).

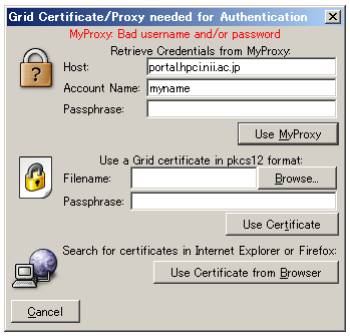


Fig. 37

Enter the correct HPCI-ID or passphrase, and try again.

(4) If you do not receive any error message, but cannot login the login server, and see the message "Disconnected" at the bottom of the screen

If you do not receive any error message, cannot login the login server, and see the message "Disconnected" at the bottom of the screen, check the following folders for old files such as the HPCI CA self-signed certificate and the Signing Policy:

OS	Folder
Windows XP	C:¥Documents and Settings¥<username>¥.globus¥certificates
Windows Vista/7	C:¥Users¥<username>¥.globus¥certificates
Unix/Linux/MacOSX	~/.globus/certificates

Delete the old files, and try again.

2.3.3. Download with Globus Toolkit

This subsection describes the procedure for downloading your Proxy Certificate using Globus Toolkit, which is produced by Globus Alliance. Please refer to section 3.2 Installing Globus Toolkit" for instructions on installing the software.

If you want to download the proxy certificate with Globus Toolkit, you first need to store the proxy certificate in the repository (refer to the section 2.2 Proxy Certificate Registration" for details).

(1) Obtain your proxy certificate from the repository.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [HPCI-ID] -t [term of validity of proxy cert(hours)]
Enter MyProxy pass phrase: ********          ←enter the passphrase of your proxy certificate
A credential has been received for user user in /tmp/x509up_u[UID].
```

If you omit the option '`-t [term of validity of proxy cert(hours)]`.', the term of validity is set to either the term of validity of the proxy certificate stored in the repository or 12 hours, whichever is shorter.

The proxy certificate is stored in the file '`/tmp/x509up_u[UID]`' by default. If you want to store it in another location, assign the file path in which you want to store the proxy certificate to the environment variable X509_USER_PROXY, and `export` or `setenv` the variable before downloading the certificate.

(2) Check the proxy certificate information.

```
user$ grid-proxy-info -f /tmp/x509up_u[UID]
subject  : /C=JP/O=NII/OU=HPCI/CN=user/CN=proxy/CN=proxy/CN=proxy/CN=proxy
issuer   : /C=JP/O=NII/OU=HPCI/CN=user/CN=proxy/CN=proxy/CN=proxy
identity : /C=JP/O=NII/OU=HPCI/CN=user
type     : full legacy globus proxy
strength : 2048 bits
path     : /tmp/x509up_u[UID]
timeleft : 11:59:54
```

Your proxy certificate download is now complete.
Refer to section "2.5 Login to the Login Server" for instructions on accessing the login server.

2.3.3.1. Troubleshooting

(1) Troubleshooting for the error message "certificate has expired."

The error message "certificate has expired." is displayed when the proxy certificate stored in the repository has expired.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [HPCI-ID] -t 1
Enter MyProxy pass phrase: ********
Failed to receive credentials.
ERROR from myproxy-server:
X509_verify_cert() failed: certificate has expired
```

Register a new proxy certificate (Refer to section "2.2 Proxy Certificate Registration" for instructions), and try again.

(2) Troubleshooting for the error message "No credentials exist for username ..."

The error message "No credentials exist for username ..." is displayed when you have run the command with an incorrect HPCI-ID.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [wrong HPCI-ID] -t 1
Enter MyProxy pass phrase: ********
Failed to receive credentials.
ERROR from myproxy-server:
No credentials exist for username "[wrong HPCI-ID]".
```

Check the HPCI-ID, and try again.

(3) Troubleshooting for the error message "Bad password"

The error message "Bad password" is displayed when you have run the command with an incorrect passphrase.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [HPCI-ID] -t 1
Enter MyProxy pass phrase: [wrong passphrase]
Failed to receive credentials.
ERROR from myproxy-server:
```

```
Bad password
invalid credential passphrase
```

Check the passphrase, and try again.

(4) Troubleshooting for the error message "Connection refused."

The error message "Connection refused." is displayed when a communications failure has occurred between your local PC and the proxy certificate repository server.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [HPCI-ID] -t 1
Unable to connect to 136.187.100.135:7512
Unable to connect to portal.hpci.nii.ac.jp
Connection refused
```

You need to communicate to the port 7512/tcp of the HPCI Certificate Issuing System. Please contact your network administrator to make sure that the port is open. When you cannot fix the problem, please contact HPCI Helpdesk (https://www.hpci-office.jp/contact/index.html).

(5) Troubleshooting for the error message "Connection timed out."

The error message "Connection timed out." is displayed when a communications failure has occurred between your local PC and the proxy certificate repository server or the proxy certificate repository server is down.

```
user$ myproxy-logon -s portal.hpci.nii.ac.jp -l [HPCI-ID] -t 1
Unable to connect to 136.187.100.135:7512
Unable to connect to portal.hpci.nii.ac.jp
Connection timed out
```

If the proxy certificate repository server is down due to the maintenance or trouble, refer to "1.1 Overview", and access an alternative system, portal-c.hpci.nii.ac.jp, instead. If the server is neither under maintenance nor in trouble, please contact your network administrator whether you can communicate to the port 7512/tcp of the HPCI Certificate Issuing System. When you cannot fix the problem, please contact HPCI Helpdesk (https://www.hpci-office.jp/contact/index.html).

2.4. Uploading the Proxy Certificate

You do not need to upload the proxy certificate to the proxy certificate repository in order to use HPCI resources, but it is possible to use your client certificate to create the proxy certificate on your local PC. You can then upload it to the repository by following the instructions below.

This section describes the procedures available for uploading the proxy certificate to the repository. Select the one that is suitable for your client environment. Not available in Windows.

OS	2.4.1 Upload with Globus Toolkit
Windows	NG
Mac OS X	OK
Linux	OK
	gcc is required

2.4.1. Upload with Globus Toolkit

This subsection describes the procedure for uploading the Proxy Certificate using the command line tool `myproxy-init`, provided by Globus Toolkit.

Refer to section "3.2 Installing Globus Toolkit" for instructions on installing the software.

Use the tool to create a proxy certificate using the client certificate on your PC, and upload it to the repository.

The following example will create and upload a proxy certificate valid for 24 hours:

```
user$ myproxy-init -s portal.hpci.nii.ac.jp -c 24
Your identity: /C=JP/O=NII/OU=HPCI/CN=user
Enter GRID pass phrase for this identity:********        ←enter the passphrase for your private key
Creating proxy ..................................... Done
Proxy Verify OK
Your proxy is valid until: Mon Jun 27 17:17:57 2011
Enter MyProxy pass phrase:********                ←enter the passphrase for upload to the repository
Verifying - Enter MyProxy pass phrase:********                ←enter the passphrase again
A proxy valid for 24 hours (1.0 days) for user user now exists on portal.hpci.nii.ac.jp.
```

If you omit the option '-c 24', the term of validity is set to 168 hours (7 days). The maximum value that you can set is the term of validity of your client certificate.

The command `myproxy-init` uses files '`~/.globus/usercert.pem`' and '`~/.globus/userkey.pem`' by default. If you want to use different files, assign the file paths of the certificate and the private key to the environment variables `X509_USER_CERT` and `X509_USER_KEY`, respectively, and `export` or `setenv` these variables before running the command.

2.4.1.1. Troubleshooting

When you encounter an error, you can obtain debugging messages by re-running the command with the additional option **`-v`**.

(1) Troubleshooting for the error message "Bad passphrase"

The error message "Bad passphrase" is displayed when you have entered an incorrect password for your client certificate.

```
user$ myproxy-init -s portal.hpci.nii.ac.jp -c 24
Your identity: /C=JP/O=NII/OU=HPCI/CN=user
Enter GRID pass phrase for this identity: ********          ←enter wrong password
Error: Couldn't read user key: Bad passphrase for key in /home/user/.globus/userkey.pem
Use -debug for further information.
grid-proxy-init failed
```

Check the password, and try again.

(2) Troubleshooting for the error message "Couldn't verify the authenticity"

The error message "Couldn't verify the authenticity" is displayed when your certificate may have expired.

```
user$ myproxy-init -s portal.hpci.nii.ac.jp -c 24
Your identity: /C=JP/O=NII/OU=HPCI/CN=user
Enter GRID pass phrase for this identity: ********
Creating proxy ..................................................... Done
Error: Couldn't verify the authenticity of the user's credential to generate a proxy from.
Use -debug for further information.
grid-proxy-init failed
```

Rerun the command with the additional -v option. The error message "The certificate has expired" will be displayed if your certificate has expired.

```
user$ myproxy-init -v -s portal.hpci.nii.ac.jp -c 24
MyProxy v5.4 22 Apr 2011 OCSP
Attempting to connect to 136.187.100.135:7512
Successfully connected to portal.hpci.nii.ac.jp:7512

User Cert File: /home/user/.globus/usercert.pem
User Key File: /home/user/.globus/userkey.pem

Trusted CA Cert Dir: /etc/grid-security/certificates

Output File: /tmp/myproxy-proxy.521.13049
Your identity: /C=JP/O=HPCI/OU=NII/CN=user
Enter GRID pass phrase for this identity:
Creating proxy ..........+++
..+++
 Done
Error: Couldn't verify the authenticity of the user's credential to generate a proxy from.
      grid_proxy_init.c:971: globus_credential: Error verifying credential: Failed to verify
credential
globus_gsi_callback_module: Could not verify credential
globus_gsi_callback_module: The certificate has expired: Credential with subject:
/C=JP/O=HPCI/OU=NII/CN=user has expired.
grid-proxy-init failed
```

Renew your client certificate, and try again.

(3) Troubleshooting for the error message "Connection timed out"

The error message "Connection timed out." is displayed when a communications failure has occurred between your local PC and the proxy certificate repository server or the proxy certificate repository server is down.

```
user$ myproxy-init -s portal.hpci.nii.ac.jp -c 24
Unable to connect to 136.187.100.135:7512
Unable to connect to portal.hpci.nii.ac.jp
Connection timed out
```

If the proxy certificate repository server is down due to the maintenance or trouble, refer to "1.1 Overview", and access an alternative system, `portal-c.hpci.nii.ac.jp`, instead. If the server is neither under

maintenance nor in trouble, please contact your network administrator whether you can communicate to the port 7512/tcp of the HPCI Certificate Issuing System. When you cannot fix the problem, please contact HPCI Helpdesk (`https://www.hpci-office.jp/contact/index.html`).

2.5. Login to the Login Server

This section describes the two procedures available for logging in to the Login Server. Select the one suitable for your client environment.

- Windows
  → Refer to section "2.5.1 Login with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)"
- Unix/Linux/MacOSX
  →Refer to section "2.5.1 Login with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)" or "2.5.2 Login with Globus Toolkit (for Unix/Linux/MacOSX)".

2.5.1. Login with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)

Java, GSI-SSHTerm and your proxy certificate must be already downloaded and installed. Refer to section "3.1 Installing GSI-SSHTerm" for instructions on installing GSI-SSHTerm, and "2.3.2 Download with GSI-SSHTerm" for downloading your proxy certificate.

- Windows
  → Run Explorer, change directory to `bin`, and double-click on the file `sshterm.bat`.
- Unix/Linux/MacOSX
  → Change directory to `bin`, run `sshterm.sh`.

GSI-SSHTerm has successfully started if the following screen appears (Fig. 38).

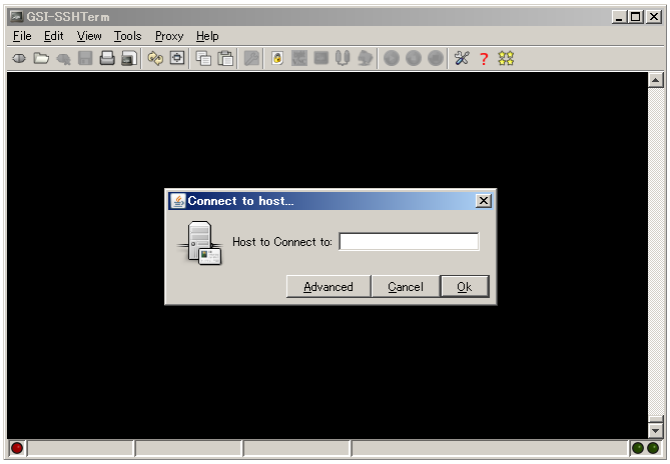


Fig. 38

If the above screen (Fig. 38) does not appear and GSI-SSHTerm does not start on Windows, check your Java settings (refer to section "3.1.1").

On the screen above (Fig. 38), enter the hostname of the login server and click the OK button to login to the login server with GSI authentication. The hostname of the login server should have been provided by the HCPI system providers that issued your HPCI local account. You do not need to click the 'Advanced' button.

If you have not yet downloaded the proxy certificate, the 'Grid Certificate/Proxy needed for Authentication' dialog appears (Fig. 39). In the dialog, enter the following information

Fig. 39

- Hostname: `portal.hpci.nii.ac.jp`
- Account Name: your HPCI-ID, not your HPCI account nor your HPCI local account
- Passphrase: the passphrase you specified when registering the proxy certificate

After you enter the correct information, click the button 'Use MyProxy'. Your proxy certificate will be automatically downloaded, and you can login to the login server.

2.5.1.1. Troubleshooting

(1) Troubleshooting for the error message "A problem occurred in loading your credentials"

The error message "A problem occurred in loading your credentials" (Fig. 40) is displayed when the downloaded proxy certificate on your client machine is corrupt.

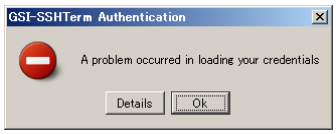


Fig. 40

Select 'Proxy > Destroy Proxy' from the menu and delete the downloaded proxy certificate from your client machine, then refer to section "2.3.2 Download with GSI-SSHTerm" and try again.

(2) If the dialog 'Grid Certificate/Proxy needed for Authentication' (Fig. 42) appears after clicking the OK button on the connection screen (Fig. 41)

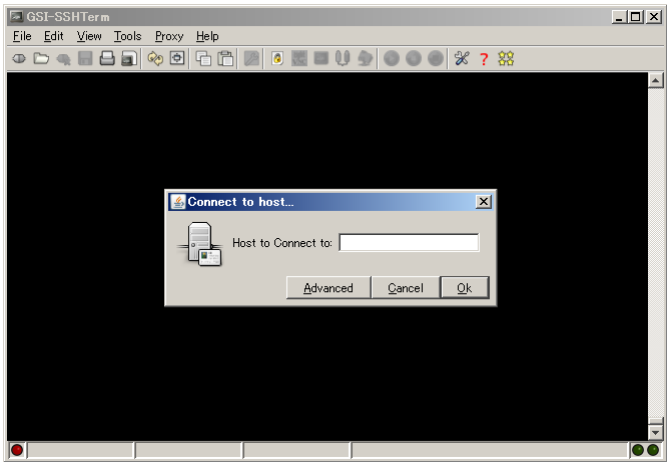


Fig. 41

Fig. 42

If the dialog 'Grid Certificate/Proxy needed for Authentication' (Fig. 42) appears after clicking the OK button on the connection screen (Fig. 41), there is no proxy certificate on your machine, or the proxy certificate on your machine has expired.

Refer to section "2.3.2 Download with GSI-SSHTerm", and try again.

(3) If you do not receive any error message, but cannot login the login server, and see the message "Disconnected" at the bottom of the screen

If you do not receive any error message, cannot login the login server, and see the message "Disconnected" at the bottom of the screen, check the following folders for old files such as the HPCI CA self-signed certificate and the Signing Policy:

OS	Folder
Windows XP	C:¥Documents and Settings¥<username>¥.globus¥certificates

Windows Vista/7	C:¥Users¥<username>¥.globus¥certificates
Unix/Linux/MacOSX	~/.globus/certificates

Delete the old files, and try again.

(4) Troubleshooting for the error message "Problem while accessing MyProxy. MyProxy get failed."

When the error message "Problem while accessing MyProxy. MyProxy get failed." (Fig. 35) is shown, refer to "2.3.2.1 Troubleshooting (1)".

2.5.2. Login with Globus Toolkit (for Unix/Linux/MacOSX)

Refer to section "3.2 Installing Globus Toolkit" for instructions on installing Globus Toolkit.

By default the command gsissh uses the file '/tmp/x509up_u[UID]' as the proxy certificate. If you store your proxy certificate in a different location, assign the certificate path to the environment variable X509_USER_PROXY, and export or setenv the variable before running the command.

(1) Obtain a proxy certificate from the proxy certificate repository.

For details, refer to section "2.3 Downloading the Proxy Certificate".

(2) Run gsissh.

```
[user@yourPC ~]$ gsissh -p 2222 [FQDN of the login server]
Last login: Mon Jul 26 12:34:56 2010 from xxx.xxx.ne.jp
[user@loginserver ~]$
```

By default gsissh enables you to connect to another login server or Gfarm storage from the server you logged in, because GSI-SSHTerm automatically creates your proxy certificate on the server you logged into (certificate creation is delegated). If you do not need to access other servers or Gfarm storage, and do not want to delegate your credential, add the option '-o GSSAPIDelegateCredentials=no'.

2.5.2.1. Troubleshooting

If you encounter the following error, rerun the command with the additional **-v** option to print debagging messages.

```
user$ gsissh -p 2222 [FQDN of Login Server]
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password,keyboard-interactive).
```

(1) Troubleshooting for an error message like "expired 0 minutes ago"

The following error means your Proxy Certificate has expired.

```
user$ gsissh -v -p 2222 [FQDN of Login Server]

...
GSS Minor Status Error Chain:
globus_gsi_gssapi: Error with gss context
globus_gsi_gssapi: Error with GSI credential
globus_gsi_gssapi: Error with gss credential handle
globus_credential: Error with credential: The proxy credential: /tmp/x509up_u[UID]
     with subject: /C=JP/O=Test University/OU=Test Unit/CN=Test User/CN=474218049
     expired 0 minutes ago.

debug1: No more authentication methods to try.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password,keyboard-interactive).
```

Renew your proxy certificate (refer to section "2.3 Downloading the Proxy Certificate" for details) , and try again.

(2) Troubleshooting for the error message "Could not find a valid proxy certificate file location"

The following error means the Proxy Certificate may have been stored in the wrong location.

```
user$ gsissh -v -p 2222 [FQDN of Login Server]

...
Attempt 2
globus_credential: Error reading proxy credential
globus_sysconfig: Could not find a valid proxy certificate file location
globus_sysconfig: Error with key filename
globus_sysconfig: File does not exist: /tmp/x509up_u[UID] is not a valid file
...
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password,keyboard-interactive).
```

Refer to section "2.3 Downloading the Proxy Certificate" for information regarding storing certificate files, save

the Proxy Certificate in /tmp/x509up_u[UID], and try again.

2.6. Transferring files to the Login Server

This section describes the two procedures available for transferring files to the Login Server. Select the one suitable for your client environment.

- Windows
  → Refer to section "2.6.1 Transfer with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)".
- Unix/Linux/MacOSX
  →Refer to "2.6.1 Transfer with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)" or "2.6.2 Transfer with Globus Toolkit (for Unix/Linux/MacOSX)".

2.6.1. Transfer with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)

Refer to 3.1 Installing GSI-SSHTerm" for instructions on installing GSI-SSHTerm if you have not installed it already.

First, start GSI-SSHTerm and connect to the login server. For details, refer to section "2.5.1 Login with GSI-SSHTerm (uses Java, for Windows/Unix/Linux/MacOSX)".

Next, select 'Tools > SFTP Session' from the menu (Fig. 43, Fig. 44).

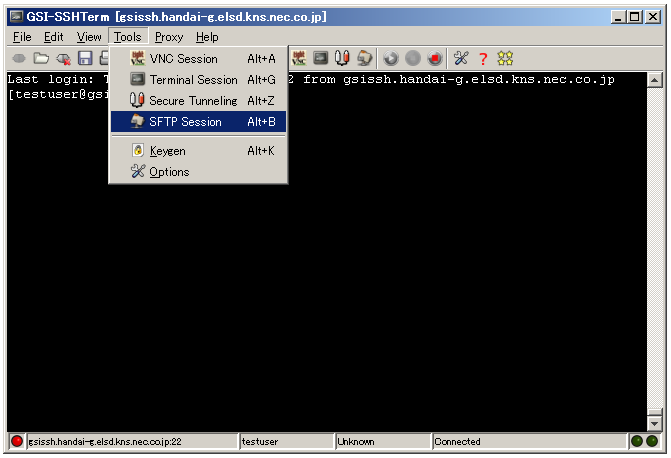


Fig. 43

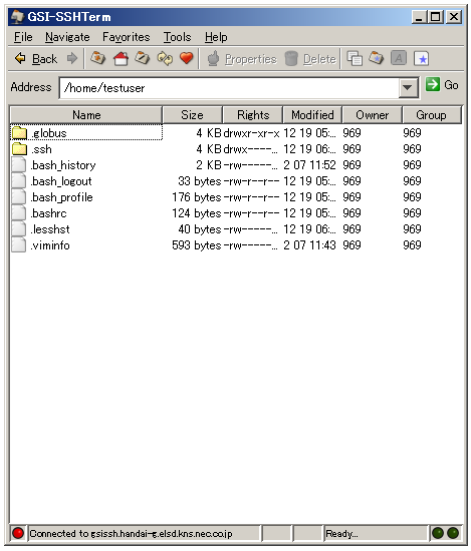


Fig. 44

A. If you want to upload a file

If you want to upload a file, select 'File > Upload File' from menu (Fig. 45).

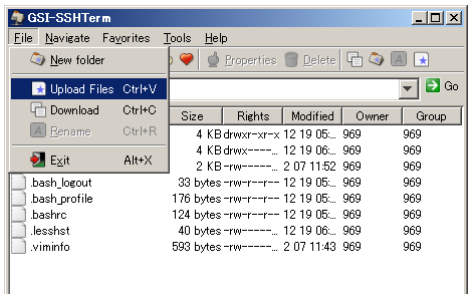


Fig. 45

The 'Select files to upload' dialog appears (Fig. 46). Select the file you want to upload, and click the Upload button (Fig. 47, Fig. 48).

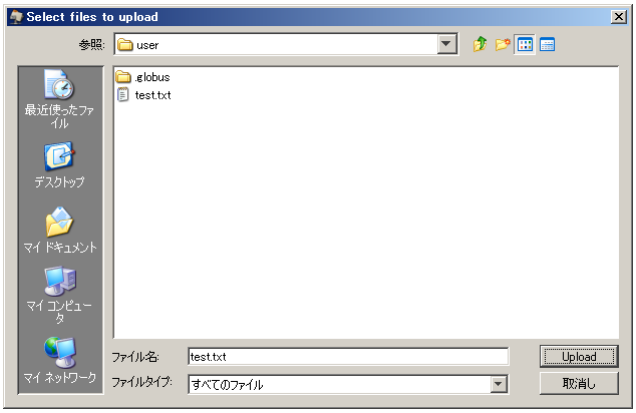


Fig. 46

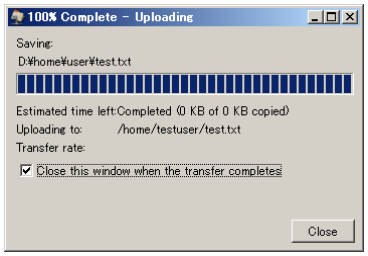


Fig. 47

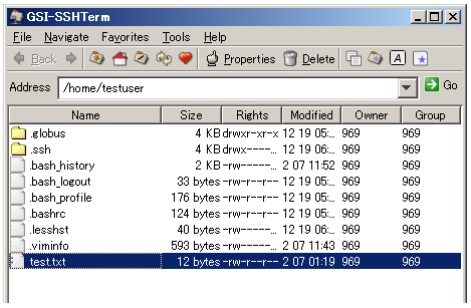


Fig. 48

Directories can be uploaded recursively.

B. If you download a file

If you want to download a file, select 'File > Download' from menu (Fig. 49).

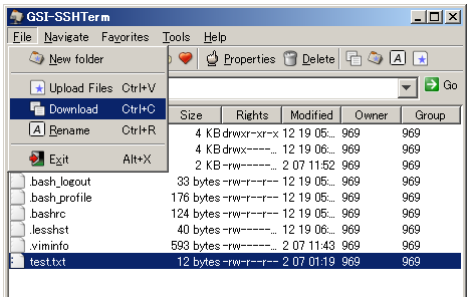


Fig. 49

The 'Select destination location' dialog appears (Fig. 50). Select the folder you want to download a file to and click the Copy button (Fig. 51, Fig. 52).

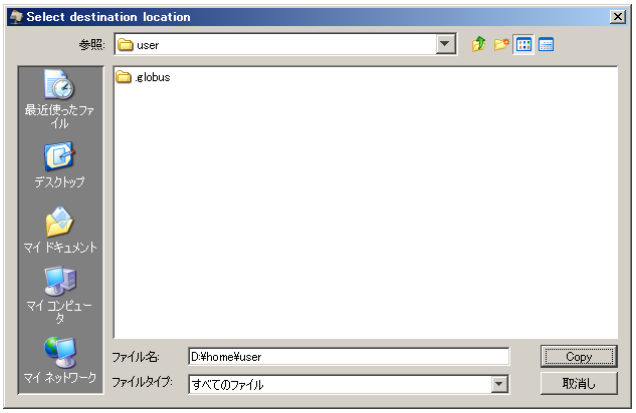


Fig. 50

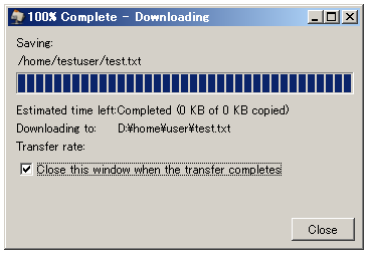


Fig. 51

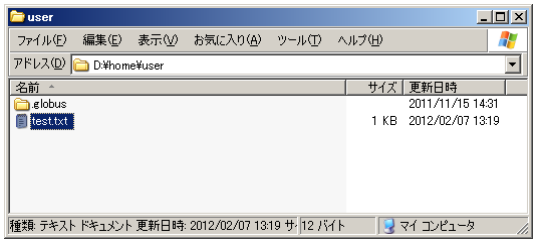


Fig. 52

Directories can be downloaded recursively.

2.6.2. Transfer with Globus Toolkit (for Unix/Linux/MacOSX)

Refer to section "3.2 Installing Globus Toolkit" for instructions on installing Globus Toolkit if you haven't installed it already.

By default the command `gsiscp` uses the file `/tmp/x509up_u[UID]` as the proxy certificate. If you store your proxy certificate in a different location, assign the certificate path to the environment variable `X509_USER_PROXY` and `export` or `setenv` the variable before running the command.

The command `gsiscp` is optimized for high performance file transfer. For details, refer to section "3.3 High performance bulk data transfer with SCP".

(1) Obtain a proxy certificate from the proxy certificate repository.

For details, refer to section "2.3 Downloading the Proxy Certificate".

(2) Transfer a file to the login server with the gsiscp command.

The port number is specified by adding option -P (upper case P)

```
user$ gsiscp -P 2222 test.txt [FQDN of the login server]:~/
test.txt                                      100%  509    0.5KB/s   0.5KB/s   00:00
```

Add option -r to copy a directory recursively.

If you want to transfer the files with the rsync command over gsissh, specify the port number with the -p option (lower case p).

```
user$ rsync -avz -e "gsissh -p 2222" test.txt [FQDN of the login server]:~/
sending incremental file list
test.txt

sent 102064 bytes  received 31bytes  2347.01 bytes/sec
total size is 104857600  speedup is 1027.06
```

If the following error occurs, your Proxy Certificate may have expired.

```
user$ gsiscp -P 2222 test.txt [FQDN of Login Server]:~/
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password,keyboard-interactive).
lost connection
```

Rerun the command with the additional option -v. If the following error message is displayed, your certificate has expired.

```
user$ gsiscp -v -P 2222 test.txt [FQDN of Login Server]:~/
...
GSS Minor Status Error Chain:
globus_gsi_gssapi: Error with gss context
globus_gsi_gssapi: Error with GSI credential
globus_gsi_gssapi: Error with gss credential handle
globus_credential: Error with credential: The proxy credential: /tmp/x509up_u[UID]
```

```
     with subject: /C=JP/O=Test University/OU=Test Unit/CN=Test User/CN=1480426253
     expired 90 minutes ago.

debug1: No more authentication methods to try.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password,keyboard-interactive).
lost connection
```

Renew your proxy certificate (refer to section "2.3 Downloading the Proxy Certificate" for details), and try again.

3. Appendix: Installing applications

3.1. Installing GSI-SSHTerm

3.1.1. Download the Software Package

(1) Download the latest GSI-SSHTerm package from the following URL.

`http://www.hpci.nii.ac.jp/software/`

The GSI-SSHTerm requires Java, so install it on your PC before installing GSI-SSHTerm.

Extract the downloaded package file, and run as follows:

- Windows
  → Run Explorer, change directory to `bin`, and double-click on the file `sshterm.bat`.
- Unix/Linux/MacOSX
  → Change directory to `bin`, run `sshterm.sh`.

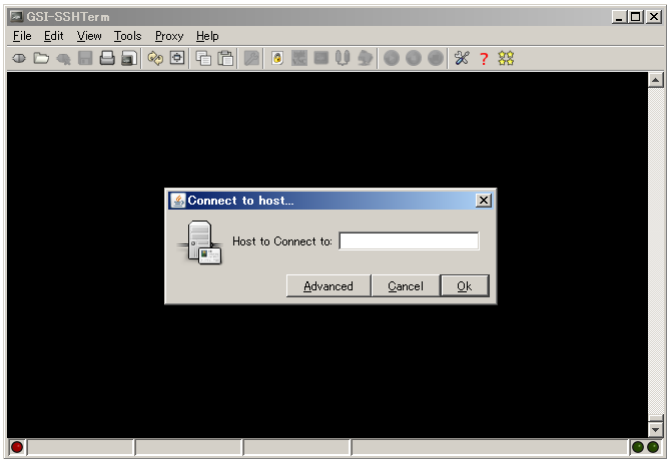


Fig. 53

GSI-SSHTerm has successfully started if the above screen appears (Fig. 53).

If the screen above (Fig. 53) does not appear and GSI-SSHTerm does not start on Windows, you may need to set the Java path.

Do one of the following, and try again:

- Assign the full pathname of the Java installation folder to the environment variable JAVA_HOME
- Assign the full pathname of the folder `bin` under the java installation folder to the environment variable PATH

For Windows, refer to the table below:

OS	Where to set
Windows XP	My Computer > Properties > Advanced > Environment variables
Windows Vista/7	Start > Control Panel > Advanced system settings > Advanced > Environment Variables

3.2. Installing Globus Toolkit

This section describes the procedure for installing Globus Toolkit.
The following are the procedures for CentOS (5, 6) and MacOSX (10.6, 10.7, 10.8.2).

3.2.1. CentOS (5, 6)

(1) Preparation

To build the Globus Toolkit from source, all of the following software should be installed.

【Required software】
- gcc
- tar
- sed
- make
- libtool-ltdl-devel
- openssl-devel
- perl
- perl-Archive-Tar (CentOS 5 only)
- perl-Compress-Zlib (CentOS 5 only)
- perl-IO-Zlib
- perl-Test-Simple
- perl-XML-Parser

(2) Download the Software Package

Download the Globus Toolkit source package from the following URL. Check the information about Globus Toolkit listed in the space of the National Institute of Informatics of HPCI Contents Management System for Information Sharing, and download the recommended version. If there is no information regarding Globus Toolkit, download the latest version.

Globus Toolkit
http://www.globus.org/toolkit/downloads/

HPCI Contents Management System for Information Sharing
https://www.hpci-office.jp/info/

In this document, we describe the installation procedure for using gt5.2.2-all-source-installer.tar.gz.

(3) Installing

Create a user 'globus' (any UID is okay).

```
% useradd -u 968 -m globus
% mkdir -p /usr/local/globus
% chown globus:globus /usr/local/globus
```

As the globus user, run the following commands:

```
% su - globus
globus$ tar zxf gt5.2.2-all-source-installer.tar.gz
globus$ cd gt5.2.2-all-source-installer
globus$ ./configure --prefix=/usr/local/globus
globus$ make gsi-openssh gsi-myproxy | tee installer.log
globus$ make install
globus$ exit

% vi /etc/profile.d/globus.sh
export GLOBUS_LOCATION=/usr/local/globus
source $GLOBUS_LOCATION/etc/globus-user-env.sh

% vi /etc/profile.d/globus.csh
setenv GLOBUS_LOCATION /usr/local/globus
source $GLOBUS_LOCATION/etc/globus-user-env.csh
```

(4) Trusting certificate issued by HPCI CA

Access the following URL via a Web browser to obtain the following files.

HPCI CA

https://www.hpci.nii.ac.jp/ca/

- HPCI CA self signed certificate
  →Select "CA Information" from the menu on the screen, and click the "HPCI CA self-signed Certificate" link to download the file hpcica.pem.zip.
- Signing Policy file
  →Select "CA Information" from the menu on the screen, and click the "Signing Policy" link to download the file hpcica.signing_policy.zip.
- CRL
  →Select "CA Information" from the menu on the screen, and click the "CRL download" link.

Create the directory to store the trusted certificates, and extract and store the retrieved files.

```
% mkdir -p ~/.globus/certificates
% cd ~/.globus/certificates
% unzip hpcica.pem.zip
% unzip hpcica.signing_policy.zip
% mv hpcica.crl `openssl crl -in hpcica.crl -noout -hash`.r0
```

For HPCI CA self-signed certificate, run the following command and check whether the output value of the fingerprint matches the one on the Web site.

```
$ openssl x509 -in [hash value].0 -noout -fingerprint -sha1
SHA1 Fingerprint=[Fingerprint]
```

HPCI CA certificates are now trusted.

You need to obtain the latest CRL at regular intervals. The following script, registered on crontab, will obtain the latest CRL and store it in the user directory automatically.

```
% vi /root/getCrl.sh
#!/bin/sh
CERTDIR=~/.globus/certificates
SERVER=www.hpci.nii.ac.jp
CRL_CA=hpcica.crl

/usr/bin/wget -P $CERTDIR http://$SERVER/ca/$CRL_CA
HASH_CA=`/usr/bin/openssl crl -in $CERTDIR/$CRL_CA -noout -hash`
/bin/mv $CERTDIR/$CRL_CA $CERTDIR/${HASH_CA}.r0

% chmod +x ~/getCrl.sh
```

```
% crontab -e
0 0 * * * /bin/sh ~/getCrl.sh
```

3.2.2. Mac OS X (10.6, 10.7, 10.8.2)

(1) Preparation

The following needs to be done to prepare for installation

- Install Xcode

Install Xcode from the App Store.

- Install Command Line Tools

Run Xcode, select Xcode > Preferences… > Downloads > Components > Command Line Tools > Install

- Create the installation directory

Create a directory for installing libtool-2.4.2 and Globus Toolkit.

```
$ mkdir $HOME/Local
```

- Install libtool-2.4.2

Download the libtool-2.4.2 source package from the following URL, and run the commands shown.
http://ftpmirror.gnu.org/libtool/

```
$ tar zxf libtool-2.4.2.tar.gz
$ cd libtool-2.4.2
$ ./configure --prefix=$HOME/Local/libtool-2.4.2
$ make
$ make install
```

(2) Download the Software Package

Refer to section "3.2.1 (2) Download the Software Package".

(3) Installing

Run the following commands:

```
$ mkdir $HOME/Local/gt5.2.2
$ export CPPFLAGS="-l$HOME/Local/libtool-2.4.2/include"
$ export LDFLAGS="-L$HOME/Local/libtool-2.4.2/lib"
$ tar zxf gt5.2.2-all-source-installer.tar.gz
$ cd gt5.2.2-all-source-installer
$ ./configure --prefix=$HOME/L丘l･gt5.2.2 --with-flavor=gcc64dbg
$ make gsi-openssh gsi-myproxy | tee installer.log

% vi $HOME/.bashrc
export GLOBUS_LOCATION=$HOME/Local/gt5.2.2
PATH=$GLOBUS_LOCATION/bin:$PATH

% vi $HOME/.bash_profile
if [ -f $HOME/.bashrc ]; then
   source $HOME/.bashrc
fi

$ source $HOME/.bashrc
$ mkdir $GLOBUS_LOCATION/etc/ssh
```

(4) Trusting certificate issued by HPCI CA

Refer to section "3.2.1 (4) Trusting certificate issued by HPCI CA".

3.3. High performance bulk data transfer with SCP

It is said that high performance data transfer with scp is difficult due to the data encryption involved when using the SSH protocol.

This difficulty is mainly caused by two factors: One is the communication delay, the other is the bottleneck caused by the cryptographic overhead. Researchers at the Pittsburgh Supercomputing Center worked to solve

these problems, and the GSI-SSH included in Globus Toolkit you installed in section 3.2 Installing Globus Toolkit" contains the results of their research.

You do not need to worry about communication delay if you use Linux, because window size is automatically optimized.

However, the bottleneck caused by the cryptographic overhead will be improved by specifying Multi-Threaded AES-CTR mode.

Run scp with the option `-oCipher=aes[128|192|256]-ctr` or `-caes[128|192|256]-ctr`.

It has been proven that this option enables data transfer speeds of over 1 Gbps even with network delays of several tens of ms.

```
http://www.psc.edu/networking/projects/hpn-ssh/mt-aes-ctr-results.gif
```

Reference:

```
http://www.psc.edu/networking/projects/hpn-ssh/faq.php
http://www.psc.edu/networking/projects/hpn-ssh/papers/a14-rapier.pdf
```

You can also use Gfarm fast staging command for high performance data transfer. Refer to the `gfpcopy` command in the document 'HPCI 共有ストレージ利用マニュアル [HPCI-ST01-001]' (P.12).

4. Glossary

・CRL (Certificate Revocation List)

A list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked.

・Globus Toolkit

An open source toolkit for building computing grids developed and provided by the Globus Alliance.

・grid-mapfile

A file containing entries mapping certificate subjects to local user names. This file can also serve as an access control list for GSI enabled services.

・GSI (Grid Security Infrastructure)

Single Sign On (SSO) framework using proxy certificates created from client certificates obtained from a Certificate Authority.

・IdP (Identity Provider)

A component of Shibboleth that provides user information.

・LDAP (Lightweight Directory Access Protocol)

A protocol used for connecting to directory services.

・Shibboleth

Authentication and Authorization architecture enabling Single Sign On (SSO) using Security Assertion Markup Language (SAML).

・SP (Service Provider)

A component of Shibboleth that gathers information about users from an IdP and uses the information to control access to protected resources

・Proxy Certificate

A short lived certificate created using a client certificate. GSI uses proxy certificates for Single Sign On (SSO).

5. Appendix

5.1. Flow of Proxy Certificate Registration and Downloading

This section explains how to register or download the proxy certificate delegated from your client certificate and private key in order to login to the HPCI environment (Fig. 54).
For details, refer to related chapters in this document.

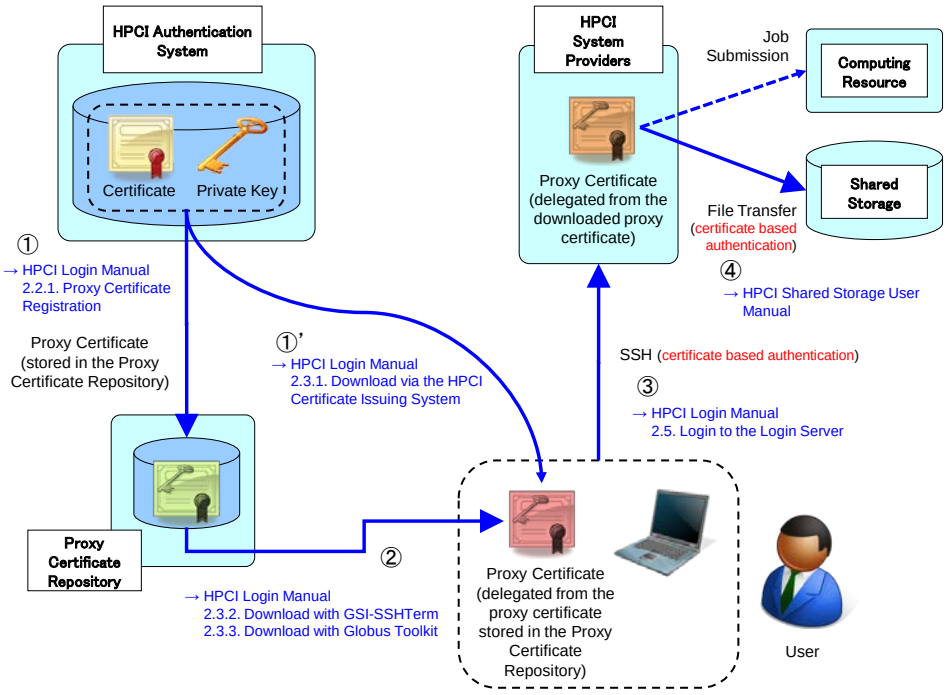


Fig. 54

① By accessing the Certificate Issuing System, you can issue a proxy certificate delegated from your client certificate and private key, and then register the proxy certificate to the Proxy Certificate Repository. Refer to "2.2.1 Proxy Certificate Registration".

② You can download the proxy certificate delegated from your proxy certificate stored in the Proxy Certificate Repository. Refer to "2.3.2 Download with GSI-SSHTerm" and "2.3.3 Download with Globus Toolkit".
Alternatively, as shown by ①' in Fig. 54, by accessing the Certificate Issuing System, you can download the proxy certificate delegated from your client certificate and private key directly to your PC. Refer to "2.3.1 Download via the HPCI Certificate Issuing System".

③ When you login to a login server of an HPCI system provider using GSI-SSHTerm, GSI-SSHTerm will automatically download the proxy certificate delegated from your proxy certificate stored in the Proxy Certificate Repository (as shown by ② in Fig. 54) to your PC and authenticate against the server with this proxy certificate. At this time, GSI-SSHTerm will store to the login server a proxy certificate delegated from the proxy certificate downloaded to your PC. Refer to "2.5 Login to the Login Server".

④ When you transfer files between the HPCI shared storage and the login server, you have to authenticate against the storage with the delegated proxy certificate on the login server. Refer to "HPCI Shared Storage User Manual".